Scott Taylor
Chief Privacy Officer
Hewlett-Packard Company
3000 Hanover St.
Palo Alto, CA 94304-1112

May 9, 2011

VIA HAND DELIVERY

United States Congress
House of Representatives
Committee on Energy and Commerce
2125 Rayburn House Office Building
Washington DC, 20515-6115

Dear Members of the House of Representatives Committee on Energy and Commerce:

Hewlett-Packard Company ("HP") respectfully and voluntarily submits this letter in response to the House of Representatives Committee on Energy and Commerce's (the "Committee") letter dated April 25, 2011 addressed to HP's Chief Executive Officer, Mr. Léo Apotheker requesting information regarding the nature of the location data, if any, that HP "smartphones" running HP's WebOS operating system track, use, store, and share.

Executive Summary

HP has provided more detailed information and specific answers below, but HP is pleased to advise the Committee that HP's WebOS devices are not configured to track location-based data without user consent. If a user does not affirmatively consent to location services during set-up or a later time, HP does not receive any location data.

Even if a user affirmatively chooses to opt in and enable location services for their WebOS device, HP does not track or maintain personalized location information. When location services are enabled by the user, HP receives anonymous location data for purposes of diagnostics and performance improvement. The location data is captured in a disaggregated manner and any device identification or personally identifiable data is decoupled from the location data when transmitted to HP. The location data received by HP is not, therefore, connected to any particular user or device.

Individuals also can choose to download 3rd party applications that may use location data. In this case, for any application that requests location data, HP devices provide notice of this request and the user is provided with a prompt for active consent to enable this sharing with the application.

Location services can be turned off easily in the menu available on the device through an on-off toggle and users are provided with a "clear my location data" option which resets their prior consents for applications to "no."

Responses to Specific Committee Questions

A. What location data do devices running your operating system track, use, store or share?

WebOS devices do not track location data that is tied to a particular user or device. Assuming the customer actively consents to using location-based services, WebOS devices are capable of determining the location of the device using a variety of means including GPS, cell tower location, and WiFi network lookup. This provides the device with an approximate location with accuracy up to about ten meters. This location data is made available to both the operating system as well as applications running on the operating system.

WebOS devices may, depending on user consent and settings, transmit anonymous location, performance, and diagnostic data to HP. These transmissions generally occur every 24 hours. The location data transmitted to HP is decoupled from any personally identifying information such as an IP address, pooled with anonymous location data for other customers, and is used by HP for purposes of diagnostics and performance improvement. The file used for these transmissions is "stored" on the WebOS device itself until it is transmitted to HP; when the transmission occurs, the file is replaced by a new one. HP does not share location data with any third-parties.

B. Why does the device track, use, store, or share that data?

WebOS devices provide location determination capability to enhance the user experience. This functionality primarily is used by applications that provide location aware capability to the user such as maps and navigation. Location data also can be used by the operating system to modify functionality based on location. For example, self-determining which country or region the device is in during device setup would permit the device to display the correct regional disclosures and notifications. WebOS also may use location information as part of diagnostics. These capabilities require the user to consent to location-based services during set-up or at some other time during ownership.

C. Where on the device is the data stored; how is it used, stored, or shared; how is it protected?

The operating system storage of location data on a WebOS device is very limited. A short-lived "cache" is sometimes employed for performance purposes. For example, location data may be stored in the "cache" while GPS is being used so that the location data can be provided on demand when requested from the GPS application. An application may choose to store the data retrieved for longer periods of time. HP does not monitor or enforce the storage of application data by third-party applications, but use of location-based services, including third-

party applications requires the user's permission. HP monitors for any user complaints and takes appropriate action if an issue arises.

When the WebOS operating system does store internal data it is stored in the internal writeable file system or within the system database. The internal file system is designed not to be accessible to third-party applications, to the user or to any desktop system. The internal database provides access control which prevents third-party applications from accessing the data. It is also not directly accessible to the user or the desktop. In the newest version of WebOS the database is encrypted using AES-128.

The data would be available to a user in developer mode which provides access to the underlying file system. The user must enable developer mode by entering a special (though common) code. Unlocked access to the device is required to enter this code. In the newest version of WebOS it is also possible set an additional passcode for the management of and access to developer mode.

D. How is that data accessible and who can access it?

The stored location data is only available to internal system components. The location determination capability can be accessed by any authorized applications. Applications can be authorized in several ways. HP internal applications are always authorized if location services are enabled. Third-party authorization depends on user configuration. If the user has configured the system to allow all applications to access location data, any application may then do so. If the user has configured the system to ask for each application before granting access to location data, the user must authorize the specific application the first (or possibly all subsequent) times the application requests access. The user is provided the opportunity to set this configuration during initial device setup and at any time later through a preference control. The user may also disable location services, or some particular types of services that will affect the ability of an application to receive this type of data.

E. Is the data automatically transferred to your company or to other devices, or to third parties? If so, how and why? Is there any other manner in which the data can be transferred to or obtained by your company, or by other devices or by third parties and, if so, how and why?

Absent affirmative user consent, location data is not automatically transferred to HP. If location services are enabled by the user, automatic transfers of anonymous location data to HP may occur during periodic performance and diagnostic data uploads to HP. The location data transmitted to HP in these transmissions is decoupled from any personally identifying information such as an IP address, pooled with anonymous location data for other customers, and is used by HP for purposes of diagnostics and performance improvement. If a user chooses to utilize a third-party application, the third-party application may transfer data it obtains.

F. *Is the user informed of, or given an opportunity to prevent, such tracking, use, storing, or sharing of data and, if so, how? Can the end user disable the tracking, use, storing or sharing of such data?*

Yes. The user is presented information regarding the location collection during device setup and provided the opportunity to disable it and set the mode in which it operates. The user can disable it at this point, prior to any contact with a remote service or collection. At any later point the user can access a preference control to modify the settings.

G. *Can the user delete the data?*

A normal user could not manually delete data just the location data stored by the operating system. He/she could, however, use one of several options provided to wipe data from the device. This would delete any locally stored location data. He/she could also delete application data by removing the application. A developer could remove the operating system data.

H. *How long does the device store the data?*

The device does not store location data long-term in the cache. If the user consents to location services, location data may be stored in the file used to transmit anonymous location, performance, and diagnostic data to HP. Transmission of the file typically occurs every 24 hours. After transmission, the file is replaced by a new file that is used for the next transmission.

I. *Sec 222 of Communications Act contains privacy provisions. Do those provisions apply to you? Should they? Does it make sense that similar information is afforded different privacy protections depending on what entity does the collecting and what service the data is collected from, especially since the entities collecting such information are increasingly competing against each other in today's information age?*

Section 222 of the Communications Act, as written, applies to telecommunications service providers. It does not appear to apply to device manufacturers, operating systems, or application/software providers. Whether Section 222 *should* be extended to apply to HP and webOS would require additional study and evaluation. That said, HP is supportive of federal legislation that would embody concepts of accountability and Privacy by Design. We are encouraged by elements of the draft Kerry Bill and believe that it is headed in the right direction.

If the Committee has any questions regarding HP's responses to the Committee's questions, please feel free to contact me at 650 857 7469.

Sincerely,

Scott M. Taylor, Chief Privacy Officer, Hewlett Packard Company